

3. (Currently Amended) The method of claim 1, wherein the fingerprint or watermark is further generated based on another self-identifier that uniquely identifies a downstream market recipient of the content. ~~associating the first set of information further comprises:~~

~~determining a self-identifier associated with the entity decrypting the content;~~

~~determining a fingerprint based, in part, on the self-identifier; and
watermarking the decrypted content employing the fingerprint.~~

4. (Currently Amended) The method of claim ~~[[3]]~~1, wherein the self-identifier is digitally signed by an encryption key associated with the entity decrypting the content.

5. (Currently Amended) The method of claim ~~[[3]]~~1, wherein the self-identifier further comprises at least one of a serial number, and a time stamp indicating approximately when the content is decrypted.

6. (Currently Amended) The method of claim 1, wherein the ~~second~~ set of information further comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the entity decrypting the content.

7. (Currently Amended) The method of claim 1, further comprising:
providing the wrapped encrypted modified content and self-identifier to a downstream market recipient;

decrypting, by the downstream market recipient, the received modified content;

further modifying the decrypted modified content by embedding another fingerprint or watermark into the modified content, wherein the other fingerprint or

12. (Currently Amended) A security device for tracing content in a highly distributed system, comprising:

- a receiver configured to receive content associated with a content owner;
- a fingerprinter-watermarker configured to perform actions including:
 - determining a self-identifier that uniquely identifies a recipient of the content;
 - ~~determining~~ generating a fingerprint ~~based, in part, on~~ from the self-identifier; and
 - watermarking the content employing the fingerprint; and
- a forensics interface configured to send information associated with the watermarked content to the content owner.

13. (Currently Amended) The security device of Claim 12, further comprising:

- a key wrap, coupled to the fingerprinter-watermarker, that is configured to perform actions, including:
 - receiving an access key associated with the recipient of the content; and
 - wrapping the content ~~and~~ together with the self-identifier employing the access key.

14. (Original) The security device of claim 13, wherein the access key is received employing an out-of-band mechanism.

15. (Original) The security device of claim 12, wherein the recipient is at least one of an aggregator, a service operator, and a user.

16. (Original) The security device of claim 12, wherein the information associated with the watermarked content comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the recipient of the content.

17. (Original) The security device of claim 12, further comprising:
a data store configured to store decrypted content; and
a fingerprinted-watermarked content data store configured to store encrypted content.

18. (Currently Amended) A network device for managing modulated data signal ~~having computer-executable instructions embodied thereon for delivering~~ content in a highly distributed system, ~~the modulated data signal comprising actions including:~~

a transceiver that is arranged to receive and to send content to another network device; and

at least one processor that is configured to execute program code to perform actions, including:

receiving a first wrapper of content from a first market participant sent to a second market participant that is associated with the network device, the wrapper including encrypted content, a first identifier that uniquely identifies the first market participant, and a content key, wherein the encrypted content, content key, and unique first identifier are together encrypted into the first wrapper using an access key associated with the network device;

decrypting the first wrapper using the access key;

decrypting the encrypted content using the decrypted content key;

generating at least one of a fingerprint or a watermark that uniquely identifies the second market participant;

marking the decrypted content by embedding the fingerprint or watermark into the decrypted content;

encrypting the marked content using the content key;

generating a second wrapper that wraps together the content key, the encrypted marked content, the first unique identifier, and a second unique identifier that uniquely identifies the second market participant, using an access key associated with a third market participant; and

transmitting the second wrapper to the third market participant.

